

specify that "the duty of the carrier upon receipt of a facially valid court order or statutorily-based authorization for an intercept extends only to the prompt and good faith execution of such court orders or authorizations."⁵²

The FBI would have the Commission limit carrier review of surveillance orders "to whether (1) the court order or certification is valid on its face (i.e., that it is what it purports to be); and, (2) the intercept is capable of being implemented as a technical matter."⁵³ Congress settled this dispute long ago when it said that a carrier would be acting in bad faith if failed "to read the order" or if it "acted beyond the scope of a court order or certification."⁵⁴ The Commission should reject any attempt to prevent carriers from carefully reviewing surveillance orders for accuracy.

3. The Scope of Carrier Liability Is Unchanged by CALEA.

The Commission requested comment on whether its proposed security rules, recordkeeping and reporting requirements would modify or mitigate carrier liability under the wiretap laws.⁵⁵

⁵² FBI Comments at 16-17.

⁵³ FBI Comments at 16-17.

⁵⁴ S. Rep. No. 99-541, at 26-27, reprinted in 1986 U.S.C.C.A.N. 3555, 3580-81 (emphasis added).

⁵⁵ NPRM ¶ 27.

Commenters argued that the Commission does not have the authority to determine the scope of the criminal law under Title 18 of the U.S. Code.⁵⁶

The FBI appears to argue that carrier concerns about incurring liability for implementing a court order containing incorrect information are misplaced.⁵⁷ The FBI states that good faith implementation of a "facially valid court order . . . all other things being equal, would provide the carrier with a defense to claims of liability."⁵⁸

CTIA is concerned that carriers may have liability, or at least be subjected to litigation, if the FBI continues to insist on implementation of its punch list as part of any standard. As the Center for Democracy and Technology pointed out in its support of the CTIA Petition for rulemaking, the privacy community views several of the punch list items as not only going beyond CALEA, but going beyond the surveillance laws.⁵⁹ Carriers, of course, have immunity when, acting in

⁵⁶ See AirTouch Comments at 27; Bell Atlantic Comments at 4; BellSouth Comments at 9; GTE Comments at 6; SBC Comments at 11; Comments of Sprint Spectrum L.P., filed December 12, 1997, at 2; USTA Comments at 7.

⁵⁷ FBI Comments at 17.

⁵⁸ FBI Comments at 17.

⁵⁹ Comments of the Center for Democracy and Technology ("CDT"), the Electronic Frontier Foundation, and Computer

good faith after review of the accuracy of the order, they implement the wiretap.⁶⁰

CTIA is concerned that if carriers provide capabilities outside the scope of CALEA, then carriers may be subject to claims that they exceeded the scope of the lawful authorization. This is particularly true given that CALEA mandates that carriers protect the privacy of communications and call-identifying information not authorized to be intercepted.⁶¹ Thus, carriers are caught between the demands of the FBI and the litigation threats of privacy groups if some of the punch list features are included in the standard.

⁶⁰ 18 U.S.C. §§ 2511, 2520.

⁶¹ 47 U.S.C. § 1002(a)(4)(A).

**III.
CONCLUSION**

CTIA urges the Commission to grant an industry-wide extension as soon as possible. The Commission should not adopt detailed carrier security procedures that are not warranted or required under CALEA. CTIA will continue its efforts to ensure a timely and cost-efficient implementation of CALEA, but the Commission ultimately is responsible for ensuring the right outcome.

Respectfully submitted,



Michael Altschul
Vice President, General Counsel

Randall S. Coleman
Vice President,
Regulatory Policy and Law

**CELLULAR TELECOMMUNICATIONS
INDUSTRY ASSOCIATION**
1250 Connecticut Ave., N.W.
Suite 200
Washington, D.C. 20036

February 11, 1998

Attachment A



Office of the Attorney General
Washington, D. C. 20530

1/23/78

Mr. Matthew J. Flanigan
President
Telecommunications Industry Association
2500 Wilson Boulevard
Suite 300
Arlington, VA 22201-3834

Dear Mr. Flanigan:

This letter responds to concerns expressed recently by members of the telecommunications industry with respect to the taking (or forbearance) of enforcement actions under the Communications Assistance for Law Enforcement Act (CALEA).

As you know, in enacting CALEA, Congress intended to preserve law enforcement's electronic surveillance capabilities and to prevent those capabilities from being eroded by technological impediments related to advanced telecommunications technologies, services, and features. To that end, Congress also specified that the solutions to overcome these impediments must be implemented within four years of the date of CALEA's enactment. The deadline for carriers to comply with section 103 of CALEA is October 25, 1998.

The Federal Bureau of Investigation (FBI) is working diligently with members of the industry, both individually and collectively, to ensure that the carriers and manufacturers are able to meet the deadline. In those situations where the carrier can foresee that it will not be able to meet the deadline because the manufacturer has yet to develop the solutions, the FBI is prepared to enter into an agreement with the manufacturer of the carrier's equipment wherein both parties (the FBI and a manufacturer) would agree upon the technological requirements and functionality for a specific switch platform (or other non-switch solution) and a reasonable and fair deployment schedule which would include verifiable milestones. In return, the Department will not pursue an enforcement action against the manufacturer or carrier as long as the terms of the agreement are met in the time frames specified. The Department will not pursue enforcement action against any carrier utilizing the switch platform (or non-switch solution) named in the agreement. Finally, the Department will support a carrier's petition to the Federal Communications

Mr. Matthew J. Flanigan
Page 2

Commission (FCC) for an extension of the compliance date for the equipment named in the agreement and for the length of time specified in the agreement. Where an agreement has been signed, if a dispute arises between the manufacturer and the FBI which cannot be resolved, the manufacturer may appeal the issue directly to the Attorney General or her designate for prompt resolution.

Your continued willingness to work toward solutions which will support law enforcement's electronic surveillance requirements is greatly appreciated.

Sincerely,

→ Signed -

Janet Reno

Attachment B



FEB 3 1998

Washington, D.C. 20530

Mr. Thomas Wheeler
President and CEO
Cellular Telecommunications Industry Association
1250 Connecticut Avenue, NW, Suite 200
Washington, DC 20036

Dear Mr. Wheeler:

This letter confirms discussions held between the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and representatives of the telecommunications industry during a January 23, 1998, meeting¹ regarding DOJ's position on the legal status under the Communications Assistance for Law Enforcement Act (CALEA) of the 11 electronic surveillance capabilities (referred to as the "punch list") that are missing from the current Telecommunications Industry Association (TIA) electronic surveillance standard J-STD-025. Additionally, it confirms the terms and conditions upon which DOJ will forbear bringing enforcement actions against industry members for non-compliance with CALEA.

"Punch List"

DOJ has reviewed the 11 "punch list" capabilities in reference to CALEA, its legislative history, and the underlying electronic surveillance statutes². In addition, DOJ reviewed a memorandum evaluating the "punch list" under CALEA that was prepared by the Office of General Counsel (OGC) of the FBI. As a result of its review, DOJ is providing the following legal opinion: 9 of the 11 capabilities are clearly within

¹Those in attendance at the January 23, 1998, meeting included representatives from the Cellular Telecommunications Industry Association (CTIA), Personal Communications Industry Association (PCIA), Telecommunications Industry Association (TIA), United States Telephone Association (USTA), Bell Atlantic, Department of Justice and the Federal Bureau of Investigation.

² CALEA was enacted to preserve the electronic surveillance capabilities of law enforcement commensurate with the legal authority found in the underlying electronic surveillance statutes, and so that electronic surveillance efforts could be conducted properly pursuant to these statutes.

review, DOJ is providing the following legal opinion: 9 of the 11 capabilities are clearly within the scope of CALEA and the underlying electronic surveillance statutes. These nine capabilities are³:

- Content of conferenced calls;
- Party Hold, Party Join, Party Drop;
- Access to subject-initiated dialing and signaling;
- Notification Message (in-band and out-of-band signaling);
- Timing to correlate call data and call content;
- Surveillance Status Message;
- Feature Status Message;
- Continuity Check; and
- Post cut-through dialing and signaling.

With respect to the first four capabilities (Content of conferenced calls; Party Hold, Party Join, Party Drop; Access to subject-initiated dialing and signaling; and Notification Message of in-band and out-of-band signaling), DOJ firmly believes that law enforcement's analysis and position regarding these assistance capability requirements satisfy CALEA section 103 requirements. These descriptions are set forth in the response submitted by the FBI⁴ to TIA Committee TR45.2 during the balloting process on standards document SP-3580A.

With respect to the fifth through the ninth capabilities (Timing to correlate call data and call content; Surveillance Status Message; Feature Status Message; Continuity Check; and Post cut-through dialing and signaling), DOJ has also concluded that law enforcement's position satisfies CALEA section 103 requirements. Because of this opinion, discussion between the industry and law enforcement will be required in order to select a mutually acceptable means of delivering the information specified by each capability. Thus, if industry disagrees with law enforcement's proposed delivery method, it must affirmatively propose a meaningful and effective alternative.

Based upon the foregoing analysis, it is DOJ's opinion that TIA interim standard J-STD-025 is failing to include and properly address the nine capabilities listed above. Industry and law enforcement may wish to act in concert to revise the interim standard J-STD-025 to include solutions for each of these missing electronic surveillance capabilities.

³ See Items 1-7, 9, and 10 of Attachment A.

⁴ The FBI is closely coordinating its efforts with state and local law enforcement representatives across the nation. In this document "law enforcement" and "FBI" refer to this partnership and are used interchangeably.

With respect to capability number eight (Standardized Delivery Interface), although a single delivery interface is not mandated by CALEA, DOJ believes that a single, standard interface would be cost effective and of great benefit to both law enforcement and telecommunications carriers. Recent productive discussions with industry have resulted in what DOJ believes is an acceptable compromise, whereby the industry would commit to a limited number of no more than five delivery interfaces. DOJ supports such an agreement.

With respect to capability number 11 (Separated Delivery), DOJ, while recognizing the usefulness of such delivery for the effectiveness of electronic surveillance, nevertheless does not believe that CALEA section 103, or the underlying electronic surveillance statutes, require separated delivery.

Building on the progress made during the final months of 1997, the FBI's CALEA Implementation Section (CIS) will continue to work with solution providers⁵ to reach an agreement on the technical feasibility of all the CALEA capability requirements.

Forbearance

During the January 23, 1998, meeting, the parties discussed the conditions under which DOJ would agree not to pursue enforcement actions against the carrier under section 108 of CALEA with regard to the CALEA mandate that a carrier meet the assistance capability requirements pursuant to CALEA section 103 by October 25, 1998, or against a manufacturer with respect to its obligation under CALEA section 106(b) to make features or modifications available on a "reasonably timely basis." A letter from the Office of the Attorney General, which was provided to all meeting attendees, outlined the basic conditions regarding forbearance:

In those situations where the carrier can foresee that it will not be able to meet the deadline because the manufacturer has yet to develop the solutions, the FBI is prepared to enter into an agreement with the manufacturer of the carrier's equipment wherein both parties (the FBI and a manufacturer) would agree upon the technological requirements and functionality for a specific switch platform (or other non-switch solution) and a reasonable and fair deployment schedule which would include verifiable milestones. In return, DOJ will not pursue an enforcement action against the manufacturer or carrier as long as the terms of the agreement are met in the time frames specified. DOJ

⁵ Solutions providers include not only switch-based manufacturers, and support service providers, but other industry entities that are engaged in the development of network-based and other CALEA-compliant solutions.

will not pursue enforcement action against any carrier utilizing the switch platform (or non-switch solution) named in the agreement.

DOJ, in consultation with the FBI, has further elaborated on the conditions related to forbearance as follows:

Any member of the telecommunications industry seeking forbearance must submit to CIS a statement that identifies the following:

1. The CALEA capability requirements that will be included in its platform or designed into any non-switch-based solution.
2. The projected date by which the platform, or non-switch-based solution, will be made commercially available, the "commercially available date."
3. A timeline for design, development, and testing milestones that will be achieved by the manufacturer from the start of the project through the commercially available date, the "milestone timeline."
4. A schedule for furnishing information to CIS at each milestone to permit CIS to verify that a milestone has been reached.
5. A list of specific types of information to be provided according to the foregoing schedule.
6. A schedule for providing mutually agreed upon data to CIS from which the Government will be able to determine the fairness and reasonableness of the CALEA solution price.
7. A list of the specific types of price-related data to be provided.

With respect to item 1, the term "CALEA capability requirements" refers to the functions defined in the TIA interim standard J-STD-025 and the first nine punch list capabilities described earlier in this letter. Law enforcement will work with each solution provider as it produces a technical feasibility study to confirm its understanding of, and ability to meet, the CALEA capability requirements. For those switching platforms, or non-switch-based solutions, on which a capability is technically infeasible, law enforcement will consult with solution providers to assess the possibility of providing effective technical alternatives that will still provide law enforcement with the necessary evidentiary and minimization data sought by the capability.

With respect to item 2, the term "commercially available date" refers to the date when the platform or non-switch-based solution

will be made available by the solution provider for the immediate purchase and deployment by a carrier. That date shall, in no event, extend beyond the first currently scheduled software generic product release after the October 25, 1998, capability compliance date. With respect to item 3, the term "milestone timeline" refers to a schedule of the necessary design, development, and testing steps to be taken by a solution provider in making a product commercially available. With respect to item 4, a solution provider is expected to include a schedule specifying the time after the completion of each milestone when CIS will be able to verify that the milestone has been reached. With respect to item 5, the specific types of information contained in the affirmative confirmation of the foregoing schedule will include, but not be limited to, draft design documents, feature specification documents, and test results. With respect to item 6, a solution provider is expected to provide a schedule detailing the delivery to CIS of all necessary information for the government to make a determination of the fairness and reasonableness of the price of the solution provider's commercially available CALEA solution. With respect to item 7, the specific types of information contained in the price-related information of the foregoing schedule will include, but not be limited to, market prices of comparable features with similar levels of design, development, and testing effort.

Forbearance for a solution provider, and its carrier customers, will be conditioned upon its ability to provide the above listed items as well as to meet verifiable solution development milestones. A solution provider's failure to meet these milestones will result in the loss of forbearance for the solution provider.

Carrier forbearance ends with the commercial availability of a solution. Switches, or portions of a network, of historical importance to law enforcement for which the government must reimburse the carrier will be identified by CIS. Equipment, facilities, and services installed or deployed after January 1, 1995, will be included in any forbearance until a solution is commercially available. Following solution availability, for those switches or portions of a network not identified by CIS, carriers are expected to follow their normal deployment processes in determining which switches, or portions of their networks, will be upgraded with the CALEA capabilities. Figure 1 illustrates the basic elements of forbearance.

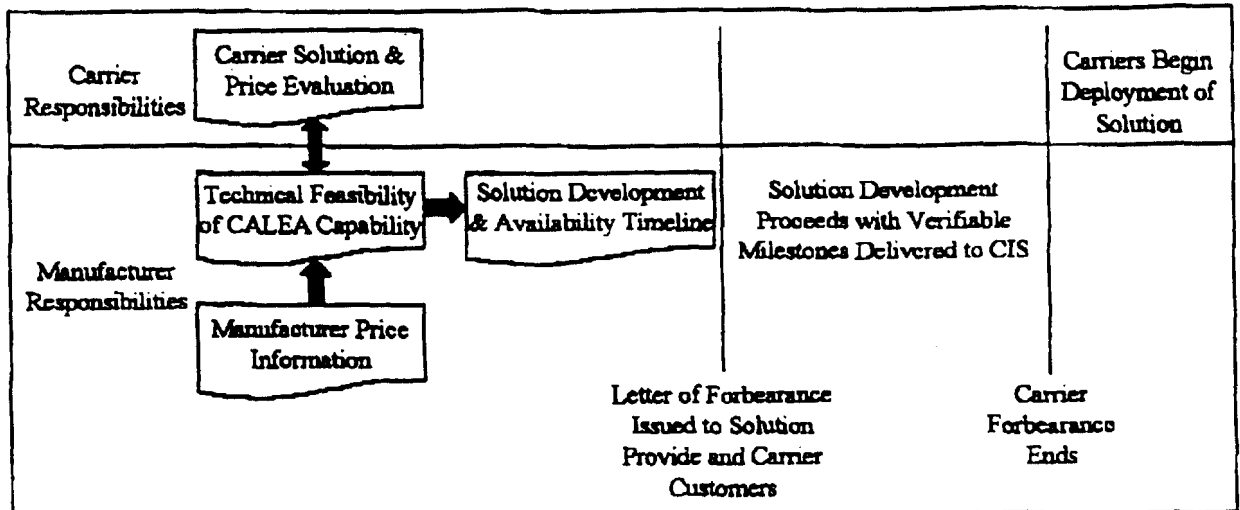


Figure 1: Forbearance

The foregoing forbearance discussion centers on two separate and distinct agreements: Agreements in Principle (AIP) between the FBI and a solution provider, and Cooperative Agreements between the FBI and a carrier.

In an AIP, the FBI and solution providers agree that solution providers have complied with the seven criteria listed above, including a feasibility analysis and pricing information for CALEA capability requirements. The feasibility analysis and pricing information will allow the government to finalize its position regarding the standard, extension of the compliance dates, forbearance, etc. The FBI, in consultation with law enforcement, will not be in a position to make critical determinations until the information described in the above seven criteria has been provided.

Currently many versions of draft AIPs are circulating, both FBI- and industry-generated, and some are more comprehensive than is presently warranted. Some of the AIPs in circulation were derived from an AIP drafted by TIA. The FBI hopes to meet with TIA during the week of February 2, 1998, to discuss the proposed AIP. The results of these discussions will then be disseminated to TIA's membership and any other interested solution provider.

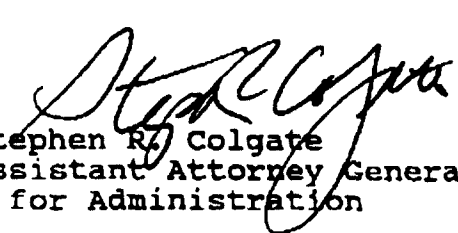
The Cooperative Agreement, on the other hand, is the contractual vehicle whereby telecommunications carriers will receive reimbursement for their eligible CALEA costs. Cooperative Agreements may be executed for different purposes at different stages of CALEA implementation. For example, an initial round of Cooperative Agreement negotiations is taking place to establish contractual vehicles whereby carriers selected to support specific solution providers with the feasibility analyses and pricing information may receive reimbursement for assisting in

this effort. Unfortunately, this initial round of negotiations has encountered some problems. One of the issues is the clarification of a carrier's role in assisting in the analysis of the solution provider's proposed solution. It appears from discussions with carriers that a mutual understanding of the intent of the government's proposed language for the Cooperative Agreements and its Statement of Work (SOW) does not yet exist. Carriers commented that the SOW included a consultative role that the carriers are unable or unwilling to perform. Although it was the government's intent to construct an SOW flexible enough to allow carriers to accommodate their normal roles in the solution provider product development process, the proposals received in response to the SOW have been too non-specific to provide real value.

The FBI still believes, and has had it confirmed by solution providers, that carriers have an essential role to play in developing the CALEA solution. The FBI will now request that each solution provider describe in detail the typical interaction it might have with one of its carrier customers during new product development. These descriptions will then be incorporated into the proposed SOWs, which the government will seek from carriers.

Your continued willingness to work with law enforcement toward the development of electronic surveillance solutions is greatly appreciated.

Sincerely,



Stephen R. Colgate
Assistant Attorney General
for Administration

ATTACHMENT A

BRIEF DESCRIPTION OF PUNCH-LIST CAPABILITIES

Number	Name	Description
1	Content of subject-initiated conference calls	Capability would enable law enforcement access to content of conference calls supported by the subject's service (including the call content of parties on hold).
2	Party Hold, Join, Drop	Messages would be sent to law enforcement that identify the active parties of a call. Specifically, on a conference call, these messages would indicate whether a party is on hold, has joined or has been dropped from the conference call.
3	Access to subject-initiated dialing and signaling	Access to all dialing and signaling information available from the subject would inform law enforcement of a subject's use of features. (Examples include the use of flash-hook, and other feature keys.)
4	In-band and out-of-band signaling (Notification Message)	A message would be sent to law enforcement when a subject's service sends a tone or other network message to the subject or associate. This can include notification that a line is ringing or busy.
5	Timing to associate call data to content	Information necessary to correlate call identifying information with the call content of a communications interception.
6	Surveillance Status Message	Message that would provide the verification that an interception is still functioning on the appropriate subject.
7	Continuity Check (C-Tone)	Electronic signal that would alert law enforcement if the facility used for delivery of call content interception has failed or lost continuity.
8	Standardized delivery interface	Would limit the number of potential delivery interfaces law enforcement would need to accommodate from the industry.
9	Feature Status Message	Message would provide affirmative notification of any change in a subject's subscribed-to features.
10	Post cut-through dialing and signaling	Information would include those digits dialed by a subject after the initial call setup is completed.
11	Separated delivery	Each party to a communication would be delivered separately to law enforcement, without combining all the voices of an intercepted (conference) call.

Attachment C

**THE CELLULAR TELECOMMUNICATIONS INDUSTRY ASSOCIATION
THE PERSONAL COMMUNICATIONS INDUSTRY ASSOCIATION
THE TELECOMMUNICATIONS INDUSTRY ASSOCIATION
THE UNITED STATES TELEPHONE ASSOCIATION**

February 10, 1998

The Honorable Stephen R. Colgate
Assistant Attorney General for Administration
U.S. Department of Justice
Tenth and Constitution Avenue, NW
Washington, DC 20530

Re: CALEA

Dear Mr. Colgate:

Thank you for your letter of February 3, 1998 regarding the Department of Justice's views on the "punch list" and the Attorney General's conditions for enforcement forbearance. Although we appreciate your efforts to elaborate on these issues, we feel that several of the items raised in your letter deserve further clarification. Depending on how these conditions are interpreted, your letter appears to place considerably more onerous requirements for an extension of time to comply than we believe CALEA requires. In fact, the conditions exceed even those in the Attorney General's letter of January 22, 1998. We are hopeful that we will be able to resolve these issues fully at our meeting on Wednesday.

Punch List

We appreciate that DOJ has reviewed the punch list and determined that at least two of the features exceed the scope of CALEA, but the conclusory verbal summary provided by the FBI at our last meeting and in your letter is not the type of "legal opinion" that we expected. As long ago as July when we first began to meet, DOJ promised an analysis of the punch list and the authority the FBI found in CALEA and other surveillance laws for imposing the punch list on industry. It was our understanding that the Department would issue a formal opinion that our attorneys could evaluate. As you might expect, such an analysis could be invaluable in helping us to better understand the Department's apparent conclusions.

Since at least last year, the industry consensus has been that CALEA does not require industry to provide these additional features. The punch list features were topics of extended discussions at meetings of the industry standards-setting body chartered to develop the safe harbor standards for CALEA.

February 10, 1998

Page 2

At those discussions, which were attended by the FBI, each of the punch list items was exhaustively documented, analyzed, determined to be outside the scope of CALEA, and, in accordance with the committee's responsibilities under law, rejected. Without a more detailed legal analysis, industry would be remiss if it were to reverse itself in the absence of citation to some form of persuasive legal authority.

For example, as we understand your letter, DOJ "firmly believes" that the first four punch list items "satisfy" CALEA Section 103. "Satisfying" CALEA and being "required" by CALEA, however, are two different things. We already have been advised by privacy advocates, as their public filings indicate, that at least one of the capabilities identified by the Department is unlawful, in their opinion. The telecommunications industry is understandably reluctant to risk millions of dollars of investments and unacceptable exposure to litigation without a better understanding of the basis of the Department's "firm belief."

Similarly, on the next five capabilities, DOJ apparently has "expressed its belief" that "law enforcement's position satisfies CALEA section 103." Again, before industry can accept such unexplained assertions we would need to see the analysis that shows that these capabilities are "required" by CALEA. For example, there seems to be no requirement in Section 103 or other law that would place an affirmative obligation on a carrier to send a message to verify that an interception is still functioning on the appropriate subject.

On this point, we are in agreement with Senator Leahy, who told the Attorney General and Director Freeh on February 4th:

I understand that at least some manufacturers and carriers have begun to design to the interim standard, but the FBI's continued insistence on the marginal 'punch list' items is only introducing further uncertainty and delay into the implementation process. Do you consider this industry interim standard to be a safe harbor "safe harbor" under section 107? If not, why have you delayed in proceeding under the statute to challenge the standard at the FCC?

As you are also well aware, CALEA provides that any person may petition the FCC to rule on standards issues should that person feel they are deficient. The FBI position appears to attempt to supplant the Federal Communications Commission ("FCC") role in the implementation of the Act.

February 10, 1998

Page 3

Forbearance

We appreciate the detailed explanation of what DOJ means by forbearance, but we believe it would be of great assistance if some of the additional "terms and conditions" could be further clarified.

First, perhaps we are misinterpreting your letter, but essentially it seems to require industry to make a number of concessions, but reserves the Department's right until after full performance by the carriers to decide whether to provide forbearance. Moreover, there appears to be a serious "timing" issue in that it is doubtful that all of the various steps you outline in your letter can be accomplished before October, 1998. Instead, we believe that forbearance, as a matter of course, should be agreed upon unconditionally if for no other reason than hundreds of carriers and vendors soon will be bringing their petitions for an extension to the FCC.

Forbearance is unnecessary when the FCC grants an extension because CALEA-compliant equipment is not available within the compliance period. As all of the parties acknowledge, compliance with the October 1998 compliance date is not achievable. Indeed, as the FBI admitted in its report to Chairman Harold Rogers, none of the major vendors will have a CALEA solution developed or available by the compliance date. Moreover, the Attorney General still has not, to this date, published a Final Notice on CALEA capacity -- years behind schedule and only eight months before CALEA's statutory compliance date. The implementation strategy outlined in your letter is also incomplete to the extent that it does not address, for example: non-priority wireline switches, non-priority GSM switches installed or deployed after January 1, 1995, as well as paging, specialized mobile radio, and others. Agreeing to a two-year extension would simply recognize these conditions. Without an extension in the near future, industry will be forced to divert much of its attention to preparing and filing extension requests at the FCC.

Second, your letter contemplates forbearance only if industry provides a CALEA solution no later than the first scheduled generic product release after October, 1998. However, as mentioned above, the FBI's report to Chairman Rogers acknowledges that most of the major manufacturers intend to phase in their solution through several upgrades. As a result, depending on what is meant by "CALEA solution," no major manufacturer may be able to satisfy this deadline.

February 10, 1998

Page 4

Third, the Department's letter proposes the establishment of a "mutually acceptable means of delivering information specified by each [law enforcement] capability." It must be remembered, however, that CALEA leaves it to industry in the first instance to decide how to implement CALEA. As you know, at CTIA's request, a new TIA project has been initiated to standardize the punch list enhanced surveillance features. At law enforcement's request, Booz-Allen Hamilton will serve as the editor of that project to develop a standard for features which are, *per se*, outside the scope of CALEA. Assigning such an important role in the standards committee to a non-TIA member (who is also a law enforcement consultant) is a clear indication of industry's good faith in this standardization process.

The enhanced surveillance services ("ESS") project was initiated to meet law enforcement's stated "needs." We do not know whether it will be technically feasible to fulfill these "needs" (as the DOJ/FBI Report to Chairman Rogers acknowledges, not all of the punch list items are feasible for all vendors), but we have undertaken this effort in good faith. We believe that the government and the telecommunications industry would benefit from standardization of these features, as standardization will yield economies of scale and scope for the potential future provision of these services.

Requiring industry to propose "meaningful and effective alternatives" before this process is completed, as your letter suggests, would simply further delay the development and deployment of CALEA compliant equipment and software. The ESS will be backward compatible with the industry standard, and, assuming that the features are technically feasible, upon payment by the government, the features can be phased in over time. In other words, law enforcement will have ample opportunity to work with industry to develop these features and thus not necessarily delay the industry's implementation of J-STD-025.

Reimbursement

Finally, your letter does not address reimbursement. Industry has attempted to engage the DOJ in a discussion of reimbursement for months now. Industry has proposed a solution whereby all equipment installed or deployed prior to the availability of CALEA-compliant technology that is not retrofitted at government expense is deemed in compliance until its next significant upgrade or major modification. This solution will allow law enforcement to spend the \$500 million authorized for CALEA on industry-wide solutions, and on areas of highest priority, while remaining secure in the knowledge that the equipment that is not retrofitted at government expense will receive CALEA features upon replacement, significant upgrade, or major modification. This solution, coupled with a revision of the CALEA effective dates, does not obligate the government to exceed the \$500 million spending cap.

February 10, 1998

Page 5

In addition, we would appreciate an opportunity to discuss the FBI's apparent reimbursement plans. For example, although not discussed in your letter, the FBI's report and our recent discussions suggest that the FBI is currently concentrating its efforts on only a few platforms and manufacturers, not an industry-wide solution. In addition, the FBI has been promoting Bell Emergis, a business unit of Bell Canada, as a provider of network-based services as an alternative to switch-based features (even though CALEA assigns the choice of solutions to each carrier, not the FBI, even when the Attorney General proposes to pay for an upgrade).

Once the solutions are commercially available, the FBI proposes to identify those portions of a carrier's network that will be targeted for upgrade. It is unclear how the FBI will make this determination and whether or not the decision will be via carrier submissions under the cost recovery rules or some other process not on the record. Also, DOJ offers to forbear from enforcement on post-January 1, 1995 installations or deployments until the solution is available, but after that, carriers are required to undertake an upgrade at their own expense in the normal upgrade schedule. In short, DOJ appears to be planning to tell carriers at the end of the process what will be reimbursed by the government and what costs will be borne by industry. Similarly, the FBI is evidently proposing to pay manufacturers to add particular punch list features to their switches, but it appears that manufacturers are being asked to agree to add the features before there has been any agreement on the amount or even the method of reimbursement. Obviously, we would appreciate greater clarification on whether our interpretation is accurate.

We appreciate the progress that has been made toward a cost-effective nationwide buyout of CALEA solutions that can be deployed on major switching platforms in areas of high priority for law enforcement. We are concerned, however, that your letter appears to shift costs of compliance to carriers, particularly small carriers deploying "non-priority" platforms. CALEA provides that carriers not reimbursed for making retrofits to their facilities are deemed in compliance with the Act.

Moving Forward

The implementation of CALEA is clearly at a crossroads. The threat of enforcement action should not be used to coerce carriers or manufacturers into contracts that are commercially unacceptable or technically infeasible. That path means only delay and possible, if not probable litigation.

February 10, 1998

Page 6

The alternative is DOJ/FBI recognition of J-STD-25 as safe harbor and acknowledgment of the ESS process as the first of many post-CALEA feature standardization efforts. Law enforcement's publication of its capacity requirements, and a revision of the CALEA effective dates in law, will allow the industry to quickly develop and deploy CALEA solutions in confidence and within the \$500 million cost ceiling established by Congress.

For over 100 years, the telecommunications industry has been a proud partner in assisting law enforcement in the execution of court-authorized electronic surveillance. In keeping with this tradition, the telecommunications industry is addressing every statutory responsibility placed upon it by CALEA. We will, in the months and years to come, continue to responsibly execute our duties under law. We hope, in the spirit of our heritage of cooperation, that at our next meeting we will be able to resolve our current misunderstandings and move forward on implementation of CALEA.

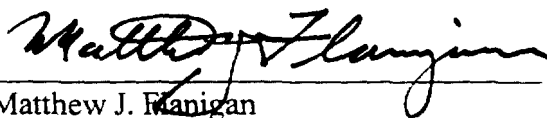
Sincerely,



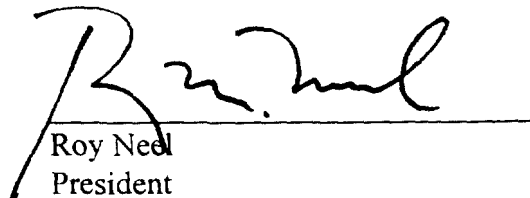
Thomas E. Wheeler
President and CEO
The Cellular Telecommunications
Industry Association



Jay Kitchen
President and CEO
The Personal Communications
Industry Association



Matthew J. Flanagan
President
The Telecommunications Industry
Association



Roy Neel
President
The United States Telephone
Association

Attachment D

**COMMUNICATIONS ASSISTANCE FOR
LAW ENFORCEMENT ACT
(CALEA)**

IMPLEMENTATION REPORT

January 26, 1998

**Prepared by:
Department of Justice
Federal Bureau of Investigation
Information Resources Division
14800 Conference Center Drive, Suite 300
Chantilly, Virginia 20151**